05-12-08

AF

IFW

PTO/SB/21 (01-08)
Approved for use through 05/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/796,599
Filing Date	March 9, 2004
First Named Inventor	Weishi Feng
Art Unit	2132
Examiner Name	Martin Jeriko P. San Juan
Total Number of Pages in This Submission	
Attorney Docket Number	MP0386

ENCLOSURES ***(check all that apply)***

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below)*:
  Response to Notice of Non-Compliant Appeal Brief (~~20~~ 19 pgs.)
  Return receipt postcard

Remarks

The Commissioner is hereby authorized to charge any additional fees that may be required under 37 CFR 1.16 or 1.17 to Deposit Account No. 08-0750. A duplicate copy of this sheet is enclosed.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Harness, Dickey & Pierce, P.L.C.		
Signature	Michael D. Wiggins		
Printed name	Michael D. Wiggins		
Date	May 9, 2008	Reg. No.	34,754

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Mary Aiello	Express Mail Label No.	EM 184 987 478 US (5/9/2008)
Signature	Mary Aiello	Date	May 9, 2008

EM 184 987 478 US

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10/796,599
Filing Date:	March 9, 2004
Applicant:	Weishi Feng
Group Art Unit:	2132
Examiner:	Martin Jeriko P. San Juan
Title:	SECURE DIGITAL CONTENT DISTRIBUTION SYSTEM AND SECURE HARD DRIVE
Attorney Docket:	MP0386

Mail Stop Appeal Brief - Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

In response to the Notice of Non-Compliant Appeal Brief mailed on April 15, 2008 please replace the Status of the Claims section of the Appeal Brief filed on April 3, 2008 with the following Status of the Claims section.

III. STATUS OF THE CLAIMS

Claims 1-83 are currently pending and are reproduced in the attached Appendix A. Each of these claims is currently pending in the application. Claims 1-83 are the claims on Appeal.

CONCLUSION

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Jeffrey J. Chapp, Reg. No. 50,579 at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17p particularly, extension of time fees.

Respectfully submitted,

Dated: 5/9/08

By: _____
Michael D. Wiggins
Reg. No. 34,754

Jeffrey J. Chapp
Reg. No. 50,579

PLEASE ADDRESS ALL CORRESPONDENCE TO:

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
Tel. No. (248) 641-1600
Fax No. (248) 641-0270
Customer No. 26703

MDW/JJC

APPENDIX A

CLAIMS APPENDED

This is a complete and current listing of the claims.

1. A secure hard drive, comprising:

a storage medium that stores encrypted digital content and corresponding encrypted content keys;

a public key decryption module that receives one of said encrypted content keys from said storage medium and that decrypts said encrypted content key using a private key and generates a content key; and

a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key,

wherein said private key is generated based on a device specific identification (ID).

2. The secure hard drive of Claim 1 wherein said storage medium is a magnetic storage medium.

3. The secure hard drive of Claim 1 wherein said public key decryption module and said block decryption module are implemented by a system on chip (SOC).

4. The secure hard drive of Claim 1 further comprising:

a content player that receives said decrypted digital content from said block decryption module and that generates at least one of an analog output signal and a digital output signal; and

an ID module that provides said device specific ID,

wherein said public key decryption module generates said private key using said device specific ID and then generates said content key based on said private key.

5. The secure hard drive of Claim 1 further comprising a controller that performs buffer management and timing of read/write operations.

6. A system comprising the secure hard drive of Claim 5 and further comprising:

an external host; and

a control interface that provides a communications interface between said controller and said external host.

7. The system of Claim 6 wherein said external host is one of a computer and a portable media player.

8. The secure hard drive of Claim 4 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark.

9. The secure hard drive of Claim 1 wherein said storage medium stores a content directory having content directory entries for said content.

10. The secure hard drive of Claim 9 wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

11. The secure hard drive of Claim 9 wherein at least one of said content directory entries contains a clear content counter that specifies a portion of said corresponding content that is not encrypted.

12. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content distributor ID field that identifies a content distributor supplying said corresponding content.

13. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content status field that has one of an active

status and a passive status, wherein said active status enables playback and said inactive status disables playback.

14. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

15. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storage medium.

16. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storage medium.

17. The secure hard drive of Claim 1 wherein said content includes at least one of audio, video, and still pictures.

18. The system of Claim 6 further comprising:

a distributed communications network;

and

a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications network.

19. The secure hard drive of Claim 1 wherein said storage medium contains encrypted content that is pre-stored thereon.

20. A secure hard drive, comprising:

a magnetic storage medium that stores encrypted digital content and corresponding encrypted content keys;

a system on chip (SOC) including:

a public key decryption module that receives one of said encrypted content keys from said magnetic storage medium and that decrypts said encrypted content key using a private key of said SOC to generate a content key; and

a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said magnetic storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key,

wherein said public key decryption module generates said private key based on a device specific identification (ID).

21. The secure hard drive of Claim 20 further comprising a content player that receives said decrypted digital content from said block decryption module and that generates an analog output signal.

22. The secure hard drive of Claim 20 further comprising a chip ID module that provides said device specific ID for said SOC, wherein said private key and a public key of said SOC are based on said chip ID.

23. The secure hard drive of Claim 20 wherein said SOC further includes a controller that performs buffer management and timing of read/write operations.

24. A system comprising the secure hard drive of Claim 23 and further comprising:

an external host; and

a control interface that provides an interface between said controller and said external host.

25. The secure hard drive of Claim 21 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark.

26. The secure hard drive of Claim 20 wherein said magnetic storage medium stores a content directory having content directory entries for said content.

27. The secure hard drive of Claim 26 wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

28. The secure hard drive of Claim 26 wherein at least one of said content directory entries contains at least one of a clear content counter that specifies a portion of said corresponding content that is not encrypted, a content distributor ID field that identifies a content distributor supplying said corresponding content, a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback, a signature field for said content distributor supplying said corresponding content, a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said magnetic storage medium, and a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said magnetic storage medium.

29. The secure hard drive of Claim 20 wherein said content includes at least one of audio, video, and still pictures.

30. The system of Claim 24 further comprising:

a distributed communications network; and

a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications system.

31. A secure hard drive, comprising:

storing means for storing encrypted digital content and corresponding encrypted content keys;

public key decryption means for receiving one of said encrypted content keys from said storing means and for decrypting said encrypted content key using a private key to generate a content key; and

block decryption means for receiving said encrypted digital content corresponding to said one of said encrypted content keys from said storing means and said content key from said public key decryption means and for decrypting said encrypted content using said content key,

wherein said private key is generated based on a device specific identification (ID).

32. The secure hard drive of Claim 31 wherein said storing means includes a magnetic storing medium.

33. The secure hard drive of Claim 31 wherein said public key decryption means and said block decryption means are implemented by a system on chip (SOC).

34. The secure hard drive of Claim 31 further comprising:

content playing means for receiving said decrypted digital content from said block decryption means and for generating at least one of an analog output signal and a digital output signal; and

an ID means for providing said device specific ID,

wherein said public key decryption means generates said private key using said device specific ID and then generates said content key based on said private key.

35. The secure hard drive of Claim 31 further comprising controller means for performing buffer management and timing of read/write operations.

36. A system comprising the secure hard drive of Claim 35 and further comprising:

an external host; and

control interface means for providing a communications interface between said controller means and said external host.

37. The system of Claim 36 wherein said external host is one of a computer and a portable media player.

38. The secure hard drive of Claim 34 further comprising watermark detecting means that communicates with an output of said content playing means for determining whether said analog signal that is output by said content playing means contains a watermark.

39. The secure hard drive of Claim 31 wherein said storing means stores a content directory having content directory entries for said content.

40. The secure hard drive of Claim 39 wherein said public key decryption means performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

41. The secure hard drive of Claim 39 wherein at least one of said content directory entries contains clear content counting means for specifying a portion of said corresponding content that is not encrypted.

42. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content distributor ID field that identifies a content distributor supplying said corresponding content.

43. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback.

44. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

45. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storing means.

46. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storing means.

47. The secure hard drive of Claim 31 wherein said content includes at least one of audio, video, and still pictures.

48. The system of Claim 36 further comprising:

distributed means for providing a distributed communications

network; and

content distributor means for transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed means.

49. The secure hard drive of Claim 31 wherein said storing means contains encrypted content that is pre-stored thereon.

50. A secure hard drive, comprising:

magnetic storing means that stores encrypted digital content and corresponding encrypted content keys;

a system on chip (SOC) including:

public key decryption means for receiving one of said encrypted content keys from said magnetic storage means and for decrypting said encrypted content key using a private key of said SOC to generate a content key; and

block decryption means for receiving said encrypted digital content corresponding to said one of said encrypted content keys from said magnetic storing means and said content key from said public key decryption means and for decrypting said encrypted content using said content key,

wherein said public key decryption module generates said private key based on a device specific identification (ID).

51. The secure hard drive of Claim 50 further comprising content playing means for receiving said decrypted digital content from said block decryption means and for generating an analog output signal.

52. The secure hard drive of Claim 50 further comprising chip ID means for providing said device specific ID for said SOC, wherein said private key and a public key of said SOC is based on said chip ID.

53. The secure hard drive of Claim 50 wherein said SOC further includes controller means for performing buffer management and timing of read/write operations.

54. A system comprising the secure hard drive of Claim 53 and further comprising:

an external host; and

control interface means provides an interface between said controller means and said external host.

55. The secure hard drive of Claim 51 further comprising watermark detecting means that communicates with an output of said content playing means for determining whether said analog signal that is output by said content playing means contains a watermark.

56. The secure hard drive of Claim 50 wherein said magnetic storage means stores a content directory having content directory entries for said content.

57. The secure hard drive of Claim 56 wherein said public key decryption means performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

58. The secure hard drive of Claim 56 wherein said content directory entries contain at least one of clear content counting means for specifying a portion of said corresponding content that is not encrypted, a content distributor ID field that identifies a content distributor supplying said corresponding content, a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback, a signature field for said content distributor supplying said corresponding content, a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said magnetic storing means, and a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said magnetic storing means.

59. The secure hard drive of Claim 50 wherein said content includes at least one of audio, video, and still pictures.

60. The system of Claim 54 further comprising:

distributed means for providing a distributed communications network; and

content distributor means for transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed means.

61. A method for distributing digital content, comprising:

(a) storing encrypted digital content and corresponding encrypted content keys on a storage medium;

(b) receiving one of said encrypted content keys from said storage medium;

(c) decrypting said encrypted content key using a private key to generate a content key;

(d) receiving said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium;

(e) decrypting said encrypted content using said content key, and

(f) generating said private key based on a device specific identification (ID).

62. The method of Claim 61 wherein said storage medium is a magnetic storing medium.

63. The method of Claim 61 further comprising generating at least one of an analog output signal and a digital output signal based on said decrypted digital content.

64. The method of Claim 61 further comprising interfacing with an external host.

65. The method of Claim 63 further comprising determining whether said analog signal contains a watermark.

66. The method of Claim 61 further comprising storing a content directory having content directory entries for said content on said storage medium.

67. The method of Claim 66 further comprising performing digital signature verification of said content directory entry corresponding to said content that is selected for play.

68. The method of Claim 66 further comprising specifying a portion of said corresponding content that is not encrypted using a clean content field in at least one of said content directory.

69. The method of Claim 66 further comprising identifying a content distributor supplying said corresponding content using a content distributor ID field in at least one of said content directory entries.

70. The method of Claim 66 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storage medium.

71. The method of Claim 66 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

72. The method of Claim 66 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storing means.

73. The method of Claim 66 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storing means.

74. The method of Claim 61 wherein said content includes at least one of audio, video, and still pictures.

75. The method of Claim 64 further comprising:

providing a distributed communications network; and

transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection from at least one content distributor to said secure hard drive via said external host and said distributed communications network.

76. The method of Claim 61 further comprising pre-storing encrypted content on said storage medium.

77. The method of Claim 61 further comprising performing steps (b), (c), (d) and (e) using a system on chip (SOC).

78. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on said device specific ID.

79. The secure hard drive of claim 78 wherein said device specific ID is an ID associated with the secure hard drive.

80. The secure hard drive of claim 78 wherein said public key decryption module generates a public key based on said private key and generates said content key based on said public key.

81. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on a device specific ID.

82. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on a chip ID.

83. The secure hard drive of claim 1 wherein said public key decryption module generates said private key based on a chip ID of the secure hard drive.